DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

November 30, 2020

MEMORANDUM FOR SENIOR EXECUTIVE TEAM

FROM: Sunita Lough
Deputy Commissioner for Services and Enforcement
Sunita B. Lough
Digitally signed by Sunita B. Lough
Date: 2020.11.24 14:23:07 -05'00'

Jeffrey J. Tribiano
Deputy Commissioner for Operations Support
Jeffrey J. Tribiano
Digitally signed by Jeffrey J. Tribiano
Date: 2020.11.24 11:55:08 -05'00'

Kevin Q. McIver
Chief of Staff
Kevin Q. McIver
Digitally signed by Kevin Q. McIver
Date: 2020.11.30 17:26:38 -05'00'

SUBJECT: Telework Equipment During Declared Emergency

This memo describes general policy decisions related to employees' needs for equipment when teleworking during a declared emergency and under an evacuation order. Except as modified by other directives, the telework principles and requirements outlined in Article 50 of the 2019 National Agreement will continue to apply during the emergency.

Information Technology Equipment Overview

Employees with management's approval and tracking are permitted to retrieve their existing assigned information technology equipment from their post of duty (POD) for use while teleworking. This includes monitors; keyboards and mice; docking stations and port-replicators; personally-assigned printers; and assistive-technology equipment. Shared equipment, including network printers, copiers, scanners, and shredders, must not be removed without explicit management approval.

To the extent that information technology equipment needs cannot be met by retrieving equipment from the office, the Information Technology organization (IT) will attempt to supply equipment in long-term, declared emergency situations where an evacuation order has been issued, in order to allow employees to remain in duty status at their telework location. Acquisition of equipment will be contingent on the availability of funding and properly documented business justifications. The current Coronavirus Disease 2019 (COVID-19) emergency will end when the pandemic is no longer a

national emergency and/or the IRS requires employees to return to the office under Optimized (normal) Operations. IT will not provide duplicative information technology equipment; but equipment required solely for the purpose of conducting mobile work (e.g., a desktop printer provided because the shared printer in the POD is inaccessible) does not constitute duplicative equipment.

Tracking removed equipment: Managers are required to keep track of equipment removed from the POD by their employees and should work with their business unit Business Systems Planning (BSP) staff to do so. IT will employ established procedures to track bar-coded equipment sent to employees (e.g., hotspots and printers), but managers are responsible for tracking equipment employees take from the POD (e.g., monitors, personally-assigned printers, scanners, etc.) and will be expected to reconcile the inventory of removed equipment when employees return to the office. In the event of an audit on the removal and return of equipment, maintaining adequate records of the equipment is imperative and will help the IRS and auditors during the audit process.

To further assist in the tracking process, IT's User and Network Services (UNS) is developing a new employee equipment profile in the profile database for equipment provided for mandatory telework under an evacuation order.

In order for IT to fulfill an equipment request, an employee's supervisor must update the employee's equipment profile record to reflect that they are approved for specific additional information technology equipment while working at home due to a declared emergency. This step is required for IT asset inventory and audit accountability purposes. The employee must then prepare, and the supervisor must approve, an OS GetServices ticket for each IT equipment item requested. IT will ship the equipment directly to the employee's home/telework location if the employee enters the accurate mailing home/telework address details in the OS GetServices ticket. More precise profiling instructions will be issued shortly.

Returning equipment: Employees will be required to return government-supplied equipment removed from the office and/or sent to them by the IRS at the end of the declared emergency. Further guidance will be provided as we get closer to lifting the current evacuation order.

Specific Equipment

Monitors: In addition to retrieving assigned monitors from their PODs and using them for telework purposes, employees may also connect their own personal monitor(s) to their IRS laptops, pursuant to current policy.

Printers & Multi-Function Devices (MFDs): Some employees have a business need for printing, scanning, or both, that is ordinarily satisfied by shared equipment in a POD. As mentioned above, employees with government-issued, personally-assigned desktop printers are permitted to retrieve them from their POD with managerial approval. Employees not otherwise profiled for a desktop printer/scanner can request such

equipment under the declared emergency through the proper management channels. Approval will be contingent on availability of funding and properly documented business justifications for each request. The security protocols outlined in Internal Revenue Manual (IRM) 6.800.2.6.2(5), *Employee Benefits, IRS Telework Program* will not be relaxed, and employees are not permitted to connect non-IRS printers to IRS laptops/computers or to transfer documents to personal devices for printing.[1]

Managers are expected to caution employees to limit printing of sensitive data to what is minimally necessary and to remind employees to secure sensitive waste until they can place it in a locked shred/burn bin at the POD. See the Telework Privacy Considerations page and the Privacy and Records Telework Policy Checklist. Encourage employees to email questions to *Privacy.

Hotspots: In declared emergency situations only, and upon a manager's request, IT will supply hotspots for employees with portable work who would otherwise be on weather and safety leave due to the lack of Internet access. The employee must certify the lack of Internet access at their home or through their personal device, and the manager must certify that the employee has at least 24 hours per week of portable work that can be performed with hotspot connectivity. Employees who telework in non-emergency situations are required to pay for their own high-speed Internet access,[2] and hotspots provided to non-telework employees must be returned upon resumption of normal operations per the *Data Call for Hotspot Internet Connectivity Need* memorandum issued to senior executives on August 26, 2020.

Shredders: The Department of the Treasury Security Manual mandates the same standards for destroying classified and Sensitive But Unclassified (SBU) materials – specifically, burning, pulping, or shredding with shredders meeting the National Security Agency (NSA) 1x5 mm standard (also known as security level P-7) or shredding to a lesser standard and later transporting for final destruction (e.g., burning, pulping, or additional shredding). Shredders meeting NSA requirements are generally only available in a POD.

Employees are responsible for the security and appropriate storage and disposition of paper materials in a telework environment, including SBU and Personally Identifiable

---

[1] According to Cybersecurity and UNS: The primary risks with using non-IRS printers are (1) the storage of IRS data, coupled with the potential for disposal of equipment with stored IRS data; and (2)the employee's home network permitting access to the printer and exfiltration of the IRS data. With security software, IRS IT can control access to and disposition of IRS laptops connected to home networks and can control access to and disposition of IRS-provided printers (ensuring no IRS data is retrievable), but IRS IT cannot control access to nor disposition of non-IRS printers.

[2] Employees who telework in non-emergency situations are required to provide high-speed Internet connectivity for their telework site, and IRS-provided hotspots will not be provided for the exclusive purpose of making an employee telework ready in non-emergency situations. IRM 6.800.2.3.1.3.4(i). Pursuant to IRM 6.800.2.3.1.6.4, the IRS is not responsible for employees' Internet costs. This applies even during the emergency when other family members' Internet use may necessitate increasing bandwidth to the telework location.

Information (PII). Such materials may be appropriately secured at home and shredded upon return to the POD. If a noncompliant shredder is used in the home or in the POD, the paper shred must be secured and collected to send for final destruction in accordance with government requirements (e.g., placed in a shred/burn bin at the POD). Returning paper to the POD for destruction may require periodic visits to the POD, and employees should coordinate any such visits with their managers.

File cabinets: The IRS supplies file cabinets to employees on long-term frequent telework, but the IRS does not provide file cabinets solely for emergency situations due to the costs involved, the difficulty returning these items to the office, and the temporary nature of an emergency. As noted above, employees who are provided a printer while teleworking during an emergency should minimize printing, secure all sensitive materials, and return materials to the POD for proper disposal.

Virtual communications: IT provides several communication and collaboration capabilities in support of a variety of virtual communications requirements. A full listing of IT collaboration capabilities can be found at IT4U along with a Decision Tree to assist employees in determining the type of collaboration capability to use for their specific business needs. As resources permit, the IRS intends to purchase additional collaborative software licenses (e.g., WebEx and Zoom) to facilitate meetings and collaboration in a telework environment during the declared emergency.

Reasonable Accommodations

Reasonable accommodations: Employees who are blind or low-vision and/or deaf or hard-of-hearing or otherwise disabled may have additional needs, and managers should e-mail *EDI Disability Branch to ensure we are providing appropriate reasonable accommodations to these employees.

Security and privacy policies

Equipment-related: Managers shall remind employees that they must follow prescribed IRS policy in IRM 10.8.26, *Information Technology (IT) Security, Government Furnished and Personal Owned Mobile Device Security Policy*, when using IRS equipment.

Paper-related: Managers shall remind employees that even when they are teleworking during a declared emergency, employees must follow the clean desk policy in IRM 10.5.1.5.1, *Privacy and Information Protection, Privacy Policy* which applies "to data left out in work areas (including those in telework and offsite locations)," particularly where non-IRS employees may have access.

Virtual communications-related: Managers shall remind employees that when they use collaboration platforms, they must follow prescribed IRS policy relating to the sharing or use of sensitive IRS data elements (e.g., PII and tax information). Additionally, managers shall urge employees to exercise precautions regarding meeting participation, specifically including the use of a passcode for meetings, use of a waiting

room prior to admittance, awareness of host controls that request screensharing or file transfers, etc. See the Online Meeting Tools section of IRM 10.5.1.6.17.2, *Privacy and Information Protection, Privacy Policy.*